

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
27 September 2007 (27.09.2007)

PCT

(10) International Publication Number  
**WO 2007/107554 A1**

(51) International Patent Classification:  
*H04L 29/06* (2006.01)

(21) International Application Number:  
PCT/EP2007/052623

(22) International Filing Date: 20 March 2007 (20.03.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
06111590.3 23 March 2006 (23.03.2006) EP

(71) Applicant and

(72) Inventor: **KRUIJSWIJK, Lucas** [NL/NL]; Dr. Herman-  
sweg 128, NL-5624 HV Eindhoven (NL).

(74) Agent: **DELTAPATENTS B.V.**; De Zaale 11, NL-5612  
AJ Eindhoven (NL).

(81) Designated States (*unless otherwise indicated, for every  
kind of national protection available*): AE, AG, AL, AM,  
AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH,

CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES,  
FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN,  
IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR,  
LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY,  
MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS,  
RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN,  
TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

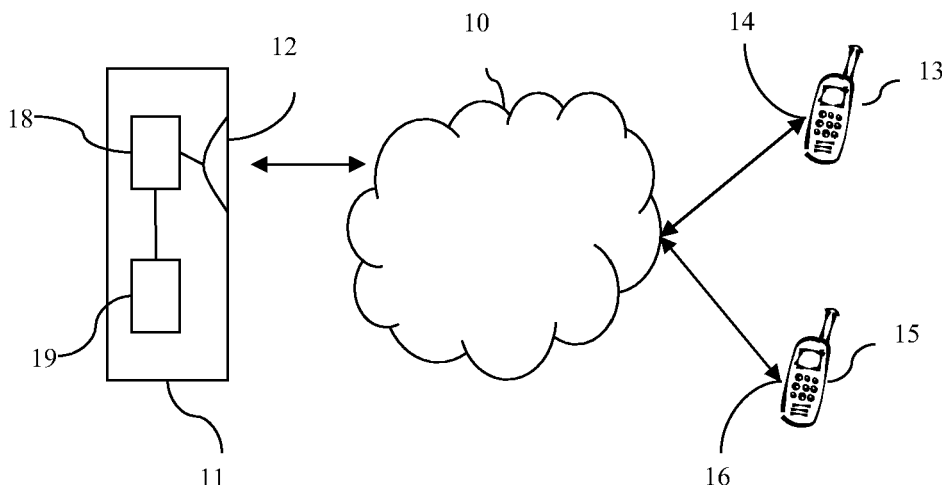
(84) Designated States (*unless otherwise indicated, for every  
kind of regional protection available*): ARIPO (BW, GH,  
GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,  
ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),  
European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,  
FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL,  
PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM,  
GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Published:**

- with international search report
- before the expiration of the time limit for amending the  
claims and to be republished in the event of receipt of  
amendments

For two-letter codes and other abbreviations, refer to the "Guid-  
ance Notes on Codes and Abbreviations" appearing at the begin-  
ning of each regular issue of the PCT Gazette.

(54) Title: COMMUNICATION SYSTEM FOR CONTROLLING USERS



(57) Abstract: A method is given for controlling users via a communication system having a server station (11) and a communication device (13) that communicate via a communication network (10). The device, for example a mobile phone, is under the control of a first user. At the server station a data base of control data is maintained. A second user is required to engage a control action at the communication device, which includes requesting to enter a personal secret code, transferring a message containing the personal secret code via the communication network to the server station, and verifying, at the server station, the personal secret code and the identity of the communication device based on the message and the control data. Furthermore, at the server station, an option is provided for a user having the secret personal code for engaging a penalty action that is detrimental to the second user. Advantageously the system allows establishing proof that the second user has in person engaged the control action at the first communication device.

WO 2007/107554 A1

## COMMUNICATION SYSTEM FOR CONTROLLING USERS.

The invention relates to a method for controlling users via a communication system, the system comprising a server station having a network interface for communicating via a communication network, and a first communication device having a network interface for communicating via the communication network,  
5 the device being under the control of a first user.

The invention further relates to a server station and a communication device for controlling users according to the method.

The invention further relates to computer program product for controlling users according to the method.

10 Communication networks, and communication devices and server station constituting a communication system, are known in various forms. Usually a communication device is under the control an individual user. For example, a mobile phone is assigned to a user and is provided with a unique identity, for example via a  
15 chip card entered in the device, usually called Subscriber Identity Module (SIM) card. The server stations in such a mobile phone network are able to detect the identity of a mobile phone that is activated. Furthermore, it is known to control particular services for the users of the communication device. For example, a mobile phone  
20 may have a voice mail service assigned for recording messages when the communication device is not in reach. For accessing the voice mail service the user of the device may be asked to enter a personal code, usually called personal identification number (PIN). Only after establishing the correctness of the PIN the voice mail service of the corresponding user is accessed. In addition, for accessing  
25 more secure services like payments, the identity of the communication device may be combined with entering a PIN, and the server station may thereby establish that the person requesting the service is using the communication device that is in possession of that person. A problem of the known communication system is that control is limited to specific services for the user that is in possession of the communication device.

It is an object of the invention to provide method of controlling users via a communication system that is more flexible and allows further control of user activities.

For this purpose, according to a first aspect of the invention, the  
5 method for controlling users as described in the opening paragraph, comprises the steps of maintaining, at the server station, a data base comprising user control data and communication device control data; requiring, at the first communication device, a second user to engage a control action, the control action comprising requesting, at the first communication device, to enter a personal secret code, transferring a  
10 message containing the personal secret code from the first communication device via the communication network to the server station, and verifying, at the server station, the personal secret code and the identity of the first communication device based on the message, the user control data and the communication device control data; and providing, at the server station, an option for a user having the secret personal code  
15 for engaging a penalty action that is detrimental to the second user, for establishing that the second user has in person engaged the control action at the first communication device.

For this purpose, according to a further aspect of the invention, the  
20 server station as described in the opening paragraph is arranged for maintaining a data base comprising user control data and communication device control data; providing an option for a user having a secret personal code of a second user for engaging a penalty action that is detrimental to a second user; and, for performing a control action, receiving a message containing the personal secret code from the first  
25 communication device via the communication network, and verifying the personal secret code and the identity of the first communication device based on the message, the user control data and the communication device control data.

For this purpose, according to a further aspect of the invention, the  
30 communication device as described in the opening paragraph is characterized in that, for performing a control action, the communication device is arranged for requesting to enter a personal secret code of a second user, and transferring a message containing the personal secret code from the first communication device via the communication network to the server station.

35

The measures have the effect that the second user has to be present at the first communication device for entering the personal secret code. In particular the second user will not be tempted to reveal his personal secret code to a different user, because the different user can subsequently perform the penalty action. This  
5 has the advantage that the second user is in effect controlled to actually go to a location where he can use the first communication device.

The invention is also based on the following recognition. From the prior art use of communication systems it may be known to identify users by  
10 requesting a code to be entered. However, in effect there is no control at all about the whereabouts of the user, as long as he has access to the communication device. The inventor has seen that in a more complex scenario, the user can be actually controlled regarding his physical presence at different locations. By providing the penalty action the inventor has achieved that the user cannot communicate his  
15 personal secret code to untrustworthy persons, and therefore must be personally present. By adjusting the penalty action, and depending on the application field of the invention, there may also be one or more trusted persons that share secret codes. Note that the invention still requires that a trusted person is physically present at the respective communication device, in particular if such device is purposely chosen to  
20 be in the control of an untrustworthy person. Such control requires the data base at the server station to be arranged for maintaining user control data regarding the identity of the users and the personal secret code assigned to each user, in combination with communication device control data for establishing the identity of the communication devices and the link between the communication devices and the  
25 respective persons controlling the devices. In particular by using mobile communication devices, the invention allows control of user activities in situations where several users need to be controlled regarding their physical location.

In an embodiment the method further comprises the step of  
30 generating, at the server station, the personal secret code, storing user control data regarding the personal secret code and the second user in the data base, and transferring the personal secret code to the second user via a second communication device having a network interface for communicating via the communication network, the second communication device being under the control of the second user. This

has the advantage that the server station is in control of distributing the personal secret code to the second user in a safe way.

In an embodiment of the method the maintaining of the data base comprises at least one of administrating a time of entering the personal secret code or of receiving the message; maintaining a number of times the personal secret code has been used; assigning or terminating validity of the personal secret code in dependence of validity conditions, in a particular case the validity conditions including a predefined time period, a number of times of use and/or allowing a one-time use. This has the advantage that further control of user actions, e.g. regarding timing and/or the number of the actions, is controlled via the communication system.

In an embodiment of the method the penalty action comprises detecting a further user that engages the penalty action, and modifying the user control data for assigning a bonus to the further user, and/or modifying the user control data for executing a penalty to the second user. The further user may be detected in any suitable way, e.g. via the communication network or in a different way. The server station subsequently modifies data to execute the penalty or award the bonus. This has the advantage that the further user will be motivated to engage the penalty action.

20

Further preferred embodiments of the method, server station, communication device and computer program product according to the invention are given in the appended claims, disclosure of which is incorporated herein by reference.

25

These and other aspects of the invention will be apparent from and elucidated further with reference to the embodiments described by way of example in the following description and with reference to the accompanying drawings, in which

Figure 1 shows a communication system,  
Figure 2 shows a method of controlling a user via a control action and a penalty action,

30

Figure 3 shows controlling a user via a communication device, and  
Figure 4 shows performing a penalty action in a communication system.

Corresponding elements in different Figures may have identical reference numerals.

35

Figure 1 shows a communication system. A communication network 10 is schematically shown, and is coupled to a server station 11 and communication devices, like a first communication device 13 and a second communication device 15, for example mobile telephones. The server station 11 has a communication interface 12 for communication with the network 10. The communication devices 13,15 have communication interfaces 14,16 for communication with the network 10. The server station further has a processor 18 operatively coupled to the communication interface 12 and a memory 19 for maintaining a data base.

The server station and communication devices are arranged for controlling users as described below in detail. Generally, the server station is arranged for maintaining a data base comprising user control data and communication device control data, providing an option for a user having a secret personal code of a second user for engaging a penalty action that is detrimental to a second user, receiving a message containing the personal secret code from the first communication device via the communication network, and verifying the personal secret code and the identity of the first communication device based on the message, the user control data and the communication device control data.

It is noted that, in the communication system, each of the communication devices is under the control of a respective user. For example mobile phones are owned and operated by the respective users, and have an identity that is detectable via the network for determining a link to a selected device. Furthermore, the communication device may be a standard communication device, or may be adapted for requesting to enter a personal secret code of a second user, and transferring a message containing the personal secret code from the first communication device via the communication network to the server station.

Figure 2 shows a method of controlling a user via a control action and a penalty action. The Figure shows the method as a sequence of steps, but in practice various steps may be performed in parallel. The method starts at node START 21 and first comprises a step DATABASE 22 which maintains, at the server station, a data base comprising user control data and communication device control

data. The user control data includes data regarding the user, such as name, identity, status, access rights, etc. In particular the database includes, for a particular user, control data corresponding to a personal secret code PSC 23, for example the personal secret code itself, and/or verification data for verifying that a code entered  
5 indeed is the personal secret code of the respective user. The communication device control data includes identity data of the communication devices, like phone numbers or serial numbers, for example corresponding to a SIM card in a mobile phone. The database can have an index on the identification code of the communication device, such that accessing the data with the identification code as key is executed fast.

10

The secret code can be stored in the database by first applying a mathematical trap-door function, or hash function. Such function can not be inverted in practice. When the secret code is checked for a control action or penalty action, the same function is applied on the code that needs to be compared. Instead of  
15 comparing the original codes, the results of the trap-door function are compared. In this way the content of the database can be fully public, while the personal secret codes remain concealed. Furthermore, for the penalty action it might be sufficient that the secret code is made public. All other persons can check the code that is made public by applying the trap-door function and comparing the result with the  
20 code in the public database.

The method is now explained for a first user that controls a first communication device, and a second user that needs to be controlled. The method includes a first branch 24 for performing a control action, and a second branch for  
25 performing a penalty action. The control action includes requiring, at the first communication device, the second user to engage a control action. The penalty action provides, at the server station, an option for a user having the secret personal code of the second user for engaging the penalty action that is detrimental to the second user. The combined availability of both the control action and the penalty  
30 action results in establishing that the second user has in person engaged the control action at the first communication device.

The control action in first branch 24 comprises the following steps for verifying, at the server station, the personal secret code and the identity of the first  
35 communication device based on the message, the user control data and the

communication device control data. First it is requested, at the first communication device, to enter a personal secret code, presumably the personal secret code of the second user. The communication device transfers a message containing the personal secret code from the first communication device via the communication network to the server station. In step RECEIVE 26 the server station receives the message. In next step VERIFY PSC 27 the server station retrieves the personal secret code from the message. It is noted that message also includes identity data of the second user, for example included in the personal secret code or as separate identity data of the second user. The personal secret code, in combination with the identity data of the second user, is verified using the user control data from the data base. In next step VERIFY CDI 28 the server station retrieves the identity of the communication device (CDI, communication device identity) that has sent the message. It is noted that a particular combination of a personal secret code and a communication device identity is detected according to a predefined user control scenario in step AWARD 29, e.g. for establishing the physical presence of the second user at the location of the first communication device under the control of first user. If one of the verification steps 27,28 fails the method is terminated at node END 35.

The penalty action in second branch 25 comprises the following steps for a user having the secret personal code of the second user for engaging the penalty action. In step REC CODE 30 the server station receives a personal secret code presumed to be of a different user than the user providing the code. The step may include requesting further data for identifying the second user, which provides a further way of controlling that the different user is aware that he is penalizing the second user. In step VERCOD 31, after establishing that the code that has been entered indeed corresponds to the personal secret code of the second user, the penalty action is continued. If the verification fails, the method is terminated at node END 35. It is noted that the user having the personal secret code may be the first user, i.e. the owner of the communication device who has acquired the personal secret code of the second user, e.g. by misbehavior or sloppiness of the second user. In general, any user having the personal secret code may engage the penalty action. However, in an embodiment of the method, the identity of the user engaging the penalty action is verified in a step IDENT 32, and may be limited according to predefined rules, e.g. to persons participating in a group. In particular the person allowed engaging the penalty action may be limited to the first user or to a user

applying the first communication device, e.g. by additionally requesting a further personal secret code and/or verifying the identity of the first communication device.

5 The penalty action may include performing step PENALTY 34, which negatively affects the status of the second user. For example certain access rights of the second user are revoked, a service level is downgraded, or the personal secret code of the second user is invalidated. Furthermore, the penalty action may include performing step BONUS 33, which awards a bonus to the different user. For example  
10 certain access rights of the second user are increased, a service level is upgraded, or a payment is made available. The BONUS step 33 may further be preceded by the step IDENT 32, which requests user data identifying the different user.

The method shown in Figure 2 may further include any of the steps described now. In an embodiment, the method may include the step of generating, at  
15 the server station, the personal secret code, e.g. a random number of a predetermined number of digits. Subsequently user control data is stored regarding the personal secret code and the second user in the data base. For example cryptographical methods may be applied for generating a pair of two numbers based on user data (e.g. name) of the user, a code and a digital signature, and distribute  
20 one as the personal secret code and store the other as control number. Subsequently the personal secret code is transferred to the second user. Several methods may be used, like mail or e-mail. However, in a more secure system, the personal secret code may be transferred via a second communication device having a network interface for communicating via the communication network, the second  
25 communication device being under the control of the second user.

In an embodiment, the method may include the step of receiving, at the server station, the personal secret code from the second user. The second user is allowed to select his personal secret code, although some codes may be  
30 inadmissible (like 4 same digits). In a more secure system, the personal secret code may be transferred via a second communication device having a network interface for communicating via the communication network, the second communication device being under the control of the second user. Like in the previous embodiment, user control data regarding the personal secret code and the second user is  
35 generated and stored in the data base.

In an embodiment, the maintaining of the data base may include administrating a time of entering the personal secret code or of receiving the message. The server station may be equipped with (or have access to) a clock, and  
5 keeps record of the time at which the personal secret code or the message arrives. Furthermore, a number of times the personal secret code has been used may be administrated, and/or validity of the personal secret code may be assigned or terminated in dependence of validity conditions. In a particular case the validity conditions may be coupled to a predefined time period, a number of times of use  
10 and/or allowing a one-time use. Furthermore, persons engaged in the control action can be predefined, e.g. by maintaining a specific control scenario in the database, which scenario may require predefined users to engage control actions at specific times, locations and/or communication devices. Also the validity of the secret code can be limited to a specific the communication device, e.g. the device of the first  
15 person.

In an embodiment, the penalty action may include detecting a further user that engages the penalty action, e.g. by requesting a name or PIN code. Subsequently the penalty may be executed by modifying the data base, e.g. by  
20 modifying the user control data for assigning a bonus to the further user, and/or modifying the user control data for executing a penalty to the second user. Furthermore, said detecting may include detecting that the further user that engages the penalty action is indeed different from the second user. In particular the different user may be required, at a further communication device, to engage a further control  
25 action, similar to the control action defined above for the second user.

In an embodiment, the method may include the step of requiring the second user to engage an identification action via a second communication device having a network interface for communicating via the communication network, the  
30 second communication device being under the control of the second user. Thereby the security of any communication with the second user is enhanced. The identification action may comprise the following steps. First, at the second communication device, the second user is requested to enter his/her second personal secret code. Next, a message containing the personal secret code is  
35 transferred from the second communication device via the communication network to

the server station. Finally, at the server station, the second personal secret code and the identity of the second communication device are verified based on the message, and the user control data and the communication device control data from the data base.

5                   In an embodiment, the method may include the step of requiring each user of a group of users to engage a control action at a respective communication device under the control of a different user of the group for establishing that a group of users are at a same location. Such group control allows detecting that all members of the group are present at a same location. For example two persons may be  
10                   required to mutually enter their personal secret code via the communication device of the other person. The group control may include taking a number of pairs out of the group, and requiring the control actions to be engaged mutually within the pair, such that any two complementary subsets of the group have at least one person in the same pair. Hence, for larger groups, the total number of control actions is reduced  
15                   (compared to exhaustive combinations of all individual users).

                  In practice, the server station and communication devices may be used as follows. The current world has many ways to communicate. Usually communication via current communication systems does not require physical  
20                   presence; hence we may speak about virtual appearance. However, there are also situations where it is required that two or more people are physically on the same place. It can be desired that there is some proof that those people were indeed on the same physical place. More specific, the situation where two (or more people) are on the same physical location should be distinguished from the situation where  
25                   the people are on different locations, but with a (possible) way to communicate. Such locations are not specifically inside a room or building, but may also be outside.

                  The invention may be applied for providing proof that persons are at the same physical location, for example a person A and a person B, and requires the following technical components:

- 30                   • A computer server.
- A network. *Person A* should have to possibility to communicate with the server by using the network.
- A communication device which can communicate with the server. The communication device is in actual control by *person B*. When the

*communication device* communicates with the *server*, it is necessary that the *server* can uniquely identify the *communication device*.

For the proof creation, a *secret code* is communicated between *person A* and the *server* via the *network*. The *secret code* may be generated by the *server*, but it might  
5 also be the case that the *secret code* comes from *person A*. The proof is created when *person A* communicates with the *server* by using the *communication device* that is in actual control of *person B*, which communication includes the *secret code*.

Figure 3 shows controlling a user via a communication device. The Figure shows server 11, and communication device 13 which is under the control of  
10 person B. Arrow 41 indicates that person A communicates via the network for acquiring a personal secret code, while the database stores corresponding user control data. Arrow 42 indicates that person A enters the personal secret code into the communication device 13 of person B. Arrow 43 indicates that the communication device 13 transfers the personal secret code in a message to the server 11 via the  
15 network. Finally, the server verifies the personal secret code and communication device identity, and, assuming the verification does not fail, provides proof of the physical presence of person A.

However, as such the above does not create a strong proof of physical  
20 contact, because *person A* could communicate (on distance) the *secret code* to *person B*. Subsequently, *person B* could communicate with the *server*, instead of *person A*. To prevent such fraud, the server provides the option for a penalty action, if *person B* knows the *secret code*. The consequence of the *penalty action* may be a *bonus* for person B and/or a *penalty* for person A

25 Figure 4 shows performing a penalty action in a communication system. First person A acquires the personal secret code as indicated above. Next person A communicates the personal secret code to person B as indicated by arrow 51. Person B may enter the personal secret code for person A in the communication  
30 device 13, but at least performs the penalty action as indicated by arrow 52. The server 11 receives the personal secret code of person A from person B, and now awards a bonus to person B and/or a penalty to person A as indicated by arrow 53.

Since *person A* is now at risk when the *secret code* is known by other  
35 people, he is forced to do the *control action* by himself. This combined with the fact

that the *communication device* is uniquely identified by the *server*, ensures the physical contact.

It is noted that, in the *penalty action*, the *secret code* must finally be  
5 compared with the *secret code* as stored in the *server*. The communication of the corrupted personal secret code to the server may be performed in any suitable way, for instance by using the *communication device*, the *network* or by human intervention.

In general the method may be applied asymmetrical. However, if  
10 *person A* is also in actual control of a communication device that can be uniquely identified by the *server*, the method may demand that both persons send their *secret codes* by the communication device of the other. This is more secure and the method becomes symmetrical. One application of the invention is to use it for safety checks that must be performed by at least two technicians. Regulations (by the company or  
15 the government) may require some kind of proof that the safety checks were really performed by the technicians. With this invention, it can be proved that the technicians were at least at the same physical position. For instance, after the repair of a railroad track, regulations may require inspection by two technicians. With the invention the mobile phones (the *communication devices*) of the technicians could be  
20 used to verify that at least both technicians are on the same place. By using standard SMS-messages, the investments to implement this invention are very low.

When the *control action* is executed, the *server* may administrate the time, the identification of the mobile phone and the *secret code*. For the *penalty*  
25 *action* the *bonus* and *penalty* should be defined. These can have a real or symbolic value. For example, in the case of rule obeying technician and a rule defying technician, the rule obeying technician may still not want to penalty the rule defying technician. However, if the invention is used in the symmetrical way, then it should be realized that the rule obeying technician is likely not to reveal his *secret code* to the  
30 rule defying technician. Because of this, the *control action* can not be executed if not both technicians are on the same place.

Another application of the invention is the proof of the delivery of goods. Suppose a postman (*person A*) has to deliver a package to a recipient  
35 (*person B*) and proof of the delivery is required. The postman has received a *secret*

code assigned to the shipment. On delivery the postman will send a SMS-message containing the *secret code* with the mobile phone (the *communication device*) of the recipient. The SMS-message may be send to a *server* in control by a third party, which is independent of the organization of the postman. If the recipient knows the *secret code*, then it can alter, extend or delete the data administrated by the third party. This is the *penalty action*. The effect is that the proof of delivery is destroyed. For the recipient this is *bonus*, while for the postman this is the *penalty*. Hence it is ensured that postman and recipient will not "optimize" delivery in such way that the physical contact between postman and recipient is not necessary anymore.

Finally, this technical invention can be used to create a real life element in a networked game, e.g. an SMS game. In general SMS-games are completely virtual and no physical contact between the players of the game is required. With the invention part of the game can be that players meet in real. The *control action* should be implemented in the rules of the game. Doing the *control action* should be advantageous for at least one of the players involved in the *control action*. Similar, the *penalty action* is implemented in the rules of the game. Doing the *penalty action* should be advantageous (the *bonus*) for the player doing the *penalty action* and disadvantageous (the *penalty*) for the player that is penalized. In games an advantage for one player may be a disadvantage for the other players. This means that if the *bonus* is explicit, the *penalty* does not need to be explicit. And vice versa, if the *penalty* is explicit, the *bonus* does not need to be explicit. Since the *control action* is administrated by the *server* and it can be part of the game that the players are required to meet at a specific moment.

Although the invention has been explained mainly by embodiments using the a mobile telephone as communication device, it may be useful as well for other communication devices like personal computers, laptops, or personal digital assistants (PDA) connected via a network like the internet. Furthermore, the examples have been elucidated for secret codes embodied by digits to be entered, but the invention can be similarly applied using other personal codes, like a secret word or phrase to be entered into the communication device.

It is noted, that in this document the word 'comprising' does not exclude the presence of other elements or steps than those listed and the word 'a' or 'an' preceding an element does not exclude the presence of a plurality of such elements, that any

reference signs do not limit the scope of the claims, that the invention may be implemented by means of both hardware and software, and that several 'means' may be represented by the same item of hardware. Further, the invention is not limited to the embodiments, and lies in each and every novel feature or combination of features

5 described above.

## CLAIMS

1. Method for controlling users via a communication system, the system comprising
  - 5                   - a server station (11) having a network interface (12) for communicating via a communication network (10),  
and
  - a first communication device (13) having a network interface (14) for communicating via the communication network, the device being under the control of a first user,  
10                characterized in that the method comprises the steps of
    - maintaining, at the server station, a data base comprising user control data and communication device control data;
    - requiring, at the first communication device, a second user to engage  
15                a control action, the control action comprising
      - requesting, at the first communication device, to enter a personal secret code,
      - transferring a message containing the personal secret code from the first communication device via the communication network to the server station,  
20                and
      - verifying, at the server station, the personal secret code and the identity of the first communication device based on the message, the user control data and the communication device control data; and
      - providing, at the server station, an option for a user having the secret  
25                personal code for engaging a penalty action that is detrimental to the second user, for establishing that the second user has in person engaged the control action at the first communication device.
2. Method as claimed in claim 1, wherein the method further comprises the step of
  - 30                - generating, at the server station, the personal secret code,
  - storing user control data regarding the personal secret code and the second user in the data base, and
  - transferring the personal secret code to the second user via a second communication device having a network interface for communicating via the

communication network, the second communication device being under the control of the second user.

3. Method as claimed in claim 1, wherein the method further comprises the step of  
5                   - receiving, at the server station, the personal secret code from the second user via a second communication device having a network interface for communicating via the communication network, the second communication device being under the control of the second user, and  
                      - storing user control data regarding the personal secret code and the  
10                   second user in the data base.
4. Method as claimed in claim 1, wherein the maintaining of the data base comprises at least one of  
                      - administrating a time of entering the personal secret code or of  
15                   receiving the message;  
                      - maintaining a number of times the personal secret code has been used;  
                      - assigning or terminating validity of the personal secret code in dependence of validity conditions, in a particular case the validity conditions  
20                   including a predefined time period, a number of times of use and/or allowing a one-time use.
5. Method as claimed in claim 1, wherein the penalty action comprises  
                      - detecting a further user that engages the penalty action, and  
25                   - modifying the user control data for assigning a bonus to the further user, and/or  
                      - modifying the user control data for executing a penalty to the second user.
- 30 6. Method as claimed in claim 5, wherein the detecting comprises  
                      - detecting that the further user that engages the penalty action is different from the second user, in a particular case by requiring, at a further communication device, the further user to engage a further control action.
- 35 7. Method as claimed in claim 1, wherein the method comprises

- requiring the second user to engage an identification action via a second communication device having a network interface for communicating via the communication network, the second communication device being under the control of the second user,

5 the identification action comprising

- requesting, at the second communication device, to enter a second personal secret code of the second user,

- transferring a message containing the personal secret code from the second communication device via the communication network to the server station, and

10

- verifying, at the server station, the second personal secret code and the identity of the second communication device based on the message, the user control data and the communication device control data.

15 8. Method as claimed in claim 1, wherein the method comprises

- requiring each user of a group of users to engage a control action at a respective communication device under the control of a different user of the group for establishing that a group of users are at a same location, in a particular case by taking at least one pair out of the group, and requiring the control actions to be engaged mutually within the pair, such that any two complementary subsets of the group have at least one person in the same pair.

20

9. Server station for controlling users according to the method of claim 1, the server station (11) having a network interface (12) for communicating via a communication network (10) with a first communication device (13) having a network interface (14) for communicating via a communication network, the device being under the control of a first user, characterized in that server station is arranged for

25

- maintaining a data base comprising user control data and communication device control data;

30

- providing an option for a user having a secret personal code of a second user for engaging a penalty action that is detrimental to a second user; and, for performing a control action,

- receiving a message containing the personal secret code from the first communication device via the communication network, and

35

- verifying the personal secret code and the identity of the first communication device based on the message, the user control data and the communication device control data.

- 5     10.    Communication device for controlling users according to the method of claim 1, the communication device (13) having a network interface (14) for communicating via a communication network (10) with a server station (11) having a network interface (12) for communicating via a communication network, the device being under the control of a first user,  
10     characterized in that, for performing a control action, the communication device is arranged for

- requesting to enter a personal secret code of a second user, and  
- transferring a message containing the personal secret code from the first communication device via the communication network to the server station.

15

11.    Computer program product for controlling users via a communication system, the system comprising

- a server station having a network interface for communicating via a communication network,

20

and

- a first communication device having a network interface for communicating via the communication network, the device being under the control of a first user,

25

characterized in that the program is operative to cause a processor at the server station to perform the method as claimed in any one of the claims 1 to 8.

1/3

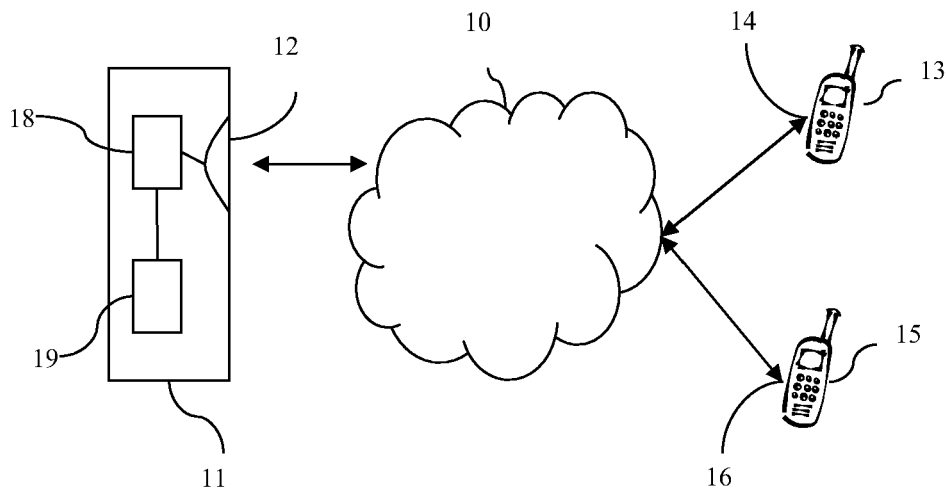


Fig. 1

2/3

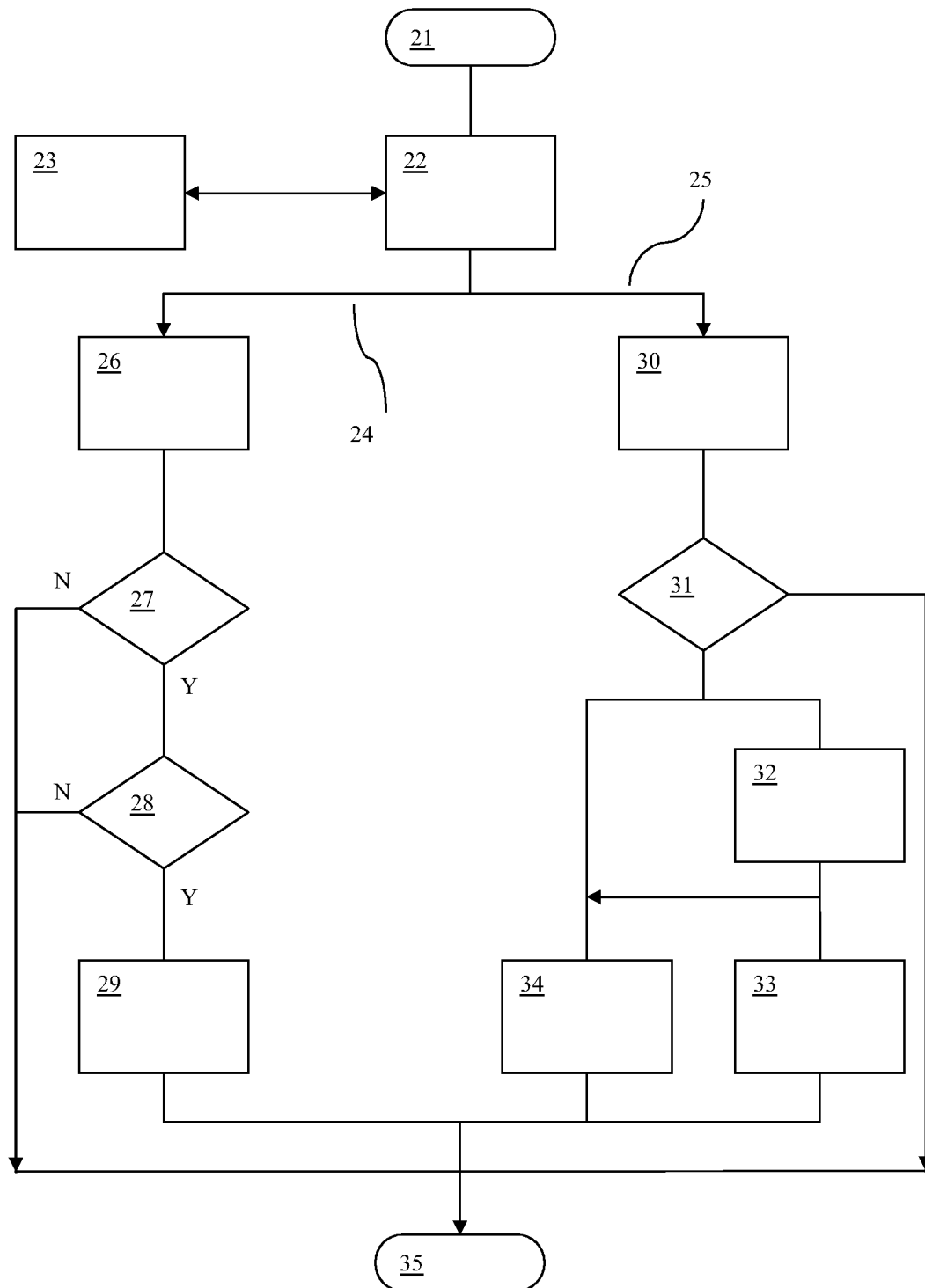


Fig. 2

3/3

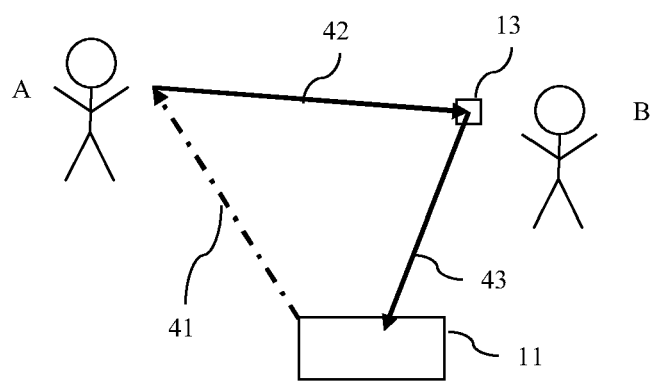


Fig. 3

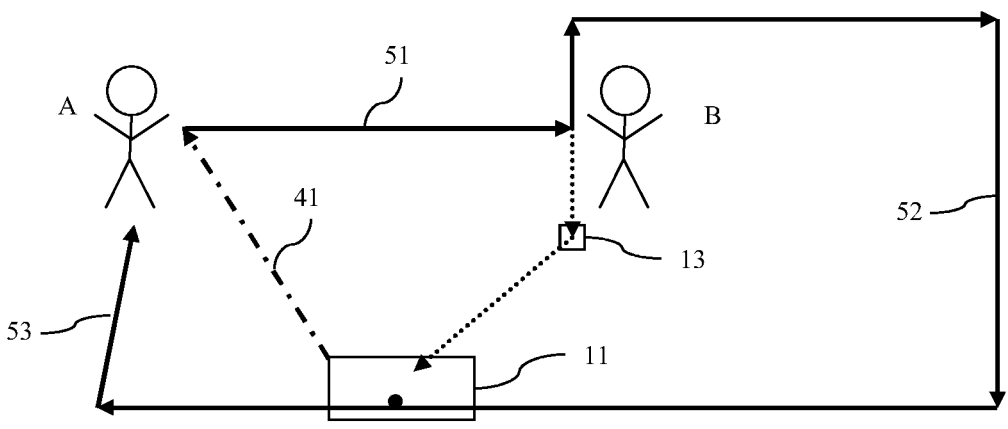


Fig. 4

# INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2007/052623

## A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, INSPEC

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                                                  | Relevant to claim No. |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| X         | JP 2005 348106 A (MITSUBISHI ELECTRIC CORP) 15 December 2005 (2005-12-15)<br>abstract<br>paragraphs [0021] - [0051]<br>figures 1-16                 | 1-10                  |
| X         | KR 2004 0025727 A (PANTECH CO LTD) 25 March 2004 (2004-03-25)<br>abstract<br>page 3, lines 2-12<br>page 3, line 37 - page 4, line 11<br>figures 1,3 | 1-10                  |



Further documents are listed in the continuation of Box C.



See patent family annex.

### \* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

9 August 2007

Date of mailing of the international search report

17/08/2007

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Bengi, Kemal

# INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2007/052623

| C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT |                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                       |
|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| Category*                                            | Citation of document, with indication, where appropriate, of the relevant passages                                                                                                                                                                                                                                                                                                                                                                           | Relevant to claim No. |
| A                                                    | <p>SEDOV I ET AL: "Security management for ad-hoc networked resource-limited mobile devices"</p> <p>VEHICULAR TECHNOLOGY CONFERENCE, 2004.</p> <p>VTC2004-FALL. 2004 IEEE 60TH LOS ANGELES, CA, USA 26-29 SEPT. 2004, PISCATAWAY, NJ, USA, IEEE, 26 September 2004 (2004-09-26), pages 3262-3266, XP010787478</p> <p>ISBN: 0-7803-8521-7</p> <p>page 3264, left-hand column, line 1 - page 3265, right-hand column, line 33</p> <p>figure 1</p> <p>-----</p> | 1-10                  |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2007/052623

| Patent document<br>cited in search report |   | Publication<br>date | Patent family<br>member(s) | Publication<br>date |
|-------------------------------------------|---|---------------------|----------------------------|---------------------|
| JP 2005348106                             | A | 15-12-2005          | NONE                       |                     |
| KR 20040025727                            | A | 25-03-2004          | NONE                       |                     |